Please type a plus sign (+) inside this box → [+]

TRANSMITTAL FORM

(to be used for all correspondence after initial filing)

Application Number	10/626,948
Filing Date	July 25, 2003
First Named Inventor	Eisentraeger
Group Art Unit	2131
Examiner Name	

Total Number of Pages in This Submission		Attorney Docket Number	MS1-1276US

ENCLOSURES   *(check all that apply)*

[ ] Fee Transmittal Form	[ ] Assignment Papers *(for an Application)*	[ ] After Allowance Communication to Group
[ ] Fee Attached	[ ] Drawing(s) Sheets	[ ] Appeal Communication to Board of Appeals and Interferences
[ ] Amendment / Reply	[ ] Licensing-related Papers	[ ] Appeal Communication to Group *(Appeal Notice, Brief, Reply Brief)*
[ ] After Final	[ ] Petition	
[ ] Affidavits/declaration(s)	[ ] Petition to Convert to a Provisional Application	[ ] Proprietary Information
[ ] Extension of Time Request	[ ] Power of Attorney, Revocation Change of Correspondence Address	[ ] Status Letter
[ ] Express Abandonment Request	[ ] Terminal Disclaimer	[✓] Other Enclosure(s) *(please identify below)*:
[✓] Information Disclosure Statement	[ ] Request for Refund	PTO-1449; 10 Non-Patent References; Return Receipt Postcard
[ ] Certified Copy of Priority Document(s)	[ ] CD, Number of CD(s) _____	
[ ] Response to Missing Parts/ Incomplete Application	**Remarks**	
[ ] Response to Missing Parts under 37 CFR 1.52 or 1.53		

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT

Firm or Individual name	Thomas A. Jolly, Reg. No. 39,241
Signature	*(signature)*
Date	3/17/2004

CERTIFICATE OF MAILING

Typed or printed name	Michelle G. Trujillo		
Signature	*(signature)* Michelle Trujillo	Date	3·17·04

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Serial No. 10/626,948
Filing Date .... Jul 25, 2003
Inventorship .... Eisentraeger
Applicant .... Microsoft Corporation
Attorney's Docket No. MS1-1276US
Title: **Squared Weil and Tate Pairing Techniques for Use with Elliptic Curves**
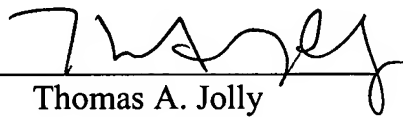
INFORMATION DISCLOSURE STATEMENT

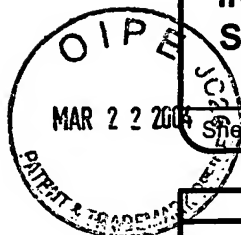*References* -- See Attached Form PTO-1449

REMARKS

The citations listed, copies attached, are submitted in compliance with the duty of disclosure defined in 37 CFR §1.56. The Examiner is requested to make these citations of official record in this application.

Respectfully Submitted,

Date: 3/17/2004

By: _____
Thomas A. Jolly
Reg. No. 39,241

Substitute for form 1449B/PTO	**Complete if Known**	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(use as many sheets as necessary)*	Application Number	10/626,948
	Filing Date	July 25, 2003
	First Named Inventor	Eisentraeger
	Group Art Unit	Not Yet Assigned
	Examiner Name	Not Yet Assigned
Sheet 1 of 1	Attorney Docket Number	MS1-1276US

NON PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No.[1]	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T[2]
		EISENTRAGER, KIRSTEN et al., "Fast Elliptic Curve Arithmetic and Improved Weil Pairing Evaluation," Topics in Cryptology, CT-RSA 2003, Marc Joye (Ed), pp. 343-354, LNCS 2612, Springer-Verlag, 2003.	
		BONEH, DAN, et al., "Identity-Based Encryption from the Weil Pairing," SIAM J. COMPUT., Vol 32, No. 3, pp. 586-615, 2003 Society for Industrial and Applied Mathematics.	
		MENEZES, ALFRED J., et al., "Reducing Elliptic Curve Logarithms to Logarithms in a Finite Field," (0018-9448/93 1993 IEEE, IEEE Transactions on Information....), 8 pages.	
		FREY, GERHARD et al., "A Remark Concerning m-Divisibility and the Discrete Logarithm in the Divisor Class Group of Curves," Mathematics of Computation, Vol. 62, No. 206, April 1994, pp. 865-874.	
		HESS, FLORIAN et al., "Two Topics in Hyperelliptic Cryptography," S. Vaudenay & A. Youssef (Eds.): SAC 2001, LNCS 2259, pp. 181-189, 2001.	
		BONEH, DAN, et al., "Short signatures from the Weil pairing," pp. 1-17.	
		GALBRAITH, STEVEN D. et al., "Implementing the Tate Pairing," Mathematics Dept., Royal Holloway, University of London, Egham, Surrey, UK & Hewlett-Packard Laboratories, Bristol, Filton Road, Stoke Gifford, Bristol, UK, pp. 1-14.	
		CANTOR, DAVID G., "Computing in the Jacobian of a Hyperelliptic Curve," Mathematics of Computation, Vol. 48, No. 177, January 1987, pp. 95-101.	
		BARRETO, PAULO S.L.M., et al., "Efficient Algorithms for Pairing-Based Cryptosystems," Universidade de Sao Paulo, Escola Politecnica, Sao Paulo (SP), Brazil & Computer Science Department, Stanford University, USA, pp. 1-16.	
		JOUX, ANTOINE, "The Weil and Tate Pairings as Building Blocks for Public Key Cryptosystems (Survey),"C. Fieker and D.R. Kohel (eds.): ANTS 2002, LNCS 2369, pp. 20-32, 2002 (Springer-Verlag Berlin Heidelberg 2002).	

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] Unique citation designation number.   [2] Applicant is to place a check mark here if English language Translation is attached.